UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,158	04/10/2007	Rached Ksontini	90500-000082/US	3063

30593 7590 11/03/2009

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
11/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,158	KSONTINI ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 September 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/577,158 is presented for examination by the examiner. Claims 21-40 are pending. Claims 21 and 39 are amended.

Response to Arguments

Applicant's arguments with respect to claims 21 and 39 have been considered but are moot in view of the new ground(s) of rejection. The amendments are alleged to support that the resources or functions are left active to the main application so it may obtain the cryptogram from the control server. This amendment does not carry full patentable weight because the activating/deactivating does not occur prior to the cryptogram reception. As presented in the claims, the relationship of cause/effect is reversed. The cryptogram is already received when the activating/deactivating occurs, so the 'effect' of the data or function being left active cannot happen before their 'cause'. It is believed the cryptogram in the last line of the independent claims should refer to future cryptograms. For prosecution on the merits, the claims will be interpreted this way. The claims would better support the arguments presented in the response filed 9/10/09, if they explicitly disclosed that the security module activates/deactivates its resources from/for use by the additional application.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 21-36 and 38-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 5,864,757 to Parker in view of USP 6,711,262 to Vatanen hereinafter Vatanen.

As per claim 21, Parker teaches a method for managing the security of at least one additional application associated to a main application with a security module of an equipment connected, via a network, to a control server managed by an operator, the main application and the additional applications use resources as data or functions stored in a security module [SIM] locally connected to said equipment, comprising the following preliminary steps:

receiving via the network, by the control server identification data comprising at least the type and software version of the equipment (col. 6, line 46) and the identity of the security module (col. 1, lines 50-55 and col. 8, lines 21-25),

analyzing and verifying by the control server of said data (col. 8, lines 26-28),

generating, by the control server, a cryptogram (col. 8 ,lines 41-44) from the result of the verification of said data,

transmitting, by the control server, the cryptogram, via network and the equipment, to the security module (col. 8, lines 60-65),

receiving and analyzing the cryptogram by the security module (col. 9, lines 50-55),

selectively activating or deactivating, by the security module, at least one resource as data or functions of said security module by executing instructions included in the cryptogram and conditioning the functioning [application to make a call] of the at one additional application according to criteria [lock/unlock] established by at least one of a supplier of said additional application, the operator, or the user of the equipment (col. 9, lines 1-8). Parker is silent in explicitly teaching wherein the resources as data or functions of the security module used by the main application are left active for connection of the equipment to the network so as to obtain the cryptogram from the control server. Again for purposes of examination, the main application is interpreted as the main calling application and the additional applications are some software programs other than the main calling application. Parker discloses locking down a phone to only emergency calls. Even in the emergency mode the phone is sill able to connect to the network. However, Vatanen teaches that resources of the SIM can be restricted from access by additional applications (col. 1, lines 50-64). Vatanen teaches that keys needed for activating and deactivating different application are stored in the SIM and can be controlled by the key list stored in the SIM (col. 2, lines 25-35, 47-60). Vatanen

teaches this is advantageous because it gives separate controls over services from the general calling network (col. 2, lines 50-55). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combined the teaching of Vatanen with those of Parker to give service provides control over not only the calling functions of a cell phone but also the applications running on them. It is also obvious that one would want to keep a cell phone on the network to allow the user to re-subscribe to additional services not directly related to making call on the network.

As per claim 22, Parker teaches the equipment is a mobile equipment of mobile telephony (see abstract).

As per claim 23, Parker teaches the network is a mobile network of the GSM, GPRS or UMTS type (col. 1, line 36).

As per claim 24, Parker teaches the security module is a subscriber module of a SIM card type inserted into the mobile equipment of mobile telephony (col. 1, line 50).

As per claim 25, Parker teaches the identification of the set mobile equipment / subscriber module is carried out from the identifier of the mobile equipment and from the identification number of the subscriber module pertaining to a subscriber to the mobile network (col. 8, lines 55-65).

As per claim 26, Parker teaches the criteria [locked/unlocked] defines the usage limits [activate / deactivate] of an application according to the risk [key exposure] associated to said application and to the type and the software version of the mobile equipment that the operator and/or the application supplier and/or the user of the mobile equipment want to take in account (col. 9, lines 2-4). Upon activating a locked phone,

Parker teaches a phone can be relocked if a key is compromised and needs to be changed. This process takes into account the identity information inside the phone, including the SIM.

As per claim 27, Parker teaches the activation method is carried out after each connection of the mobile equipment to the network (col. 9, line 11). A check is made at turn on to see if the device is locked. It does however bypass the rest of the activation method and goes to the authentication part of the method if the check is satisfied.

As per claim 28, Parker teaches the activation method is carried out after each of updating the software version of the mobile equipment (col. 9, lines 1-5). Anytime the phone receives a new subscriber identification code it is necessary for the handset to re-register with the base station.

As per claim 29, Parker teaches the activation method is carried out after each activation or deactivation of an application on the mobile equipment (col. 9, lines 1-5).

As per claim 30, Parker teaches the activation method is carried out after each updating of the software version of the subscriber module (col. 9, lines 1-5). Anytime the phone receives a new subscriber identification code it is necessary for the handset to re-register with the base station.

As per claim 31, Parker teaches the activation method is out after each updating of the resources on the subscriber module (col. 9, lines 1-5). Anytime the phone receives a new subscriber identification code it is necessary for the handset to re-register with the base station.

As per claim 32, Parker teaches the activation method is carried out periodically at a rate [each startup] given by the control server (col. 9, line 11).

As per claim 33, Parker teaches the activation method is carried out after each initialization of an application on the mobile application (col. 9, lines 1-5). Activation is synonymous with initialization.

As per claim 34, Parker teaches the subscriber module, prior to the execution of the instructions given by the cryptogram, compares the identifier of the mobile equipment with that previously received (Fig. 5, 172).

As per claim 35, Parker teaches the control server, prior to the transmission of the cryptogram, compares the identifier of the mobile equipment with that previously received and only initiates the verification operation if the identifier has changed (col. 8, lines 55-65). This activation is only done a second time if the SIM or any of its values change. Otherwise, the server already knows the phone is ok and does not send it a new IMSI.

As per claim 36, Parker teaches the cryptogram is made up of a message encrypted by the control server with the aid of an asymmetrical or symmetrical encryption key from a data set containing, among other data, the identifier of the mobile equipment, the identification number of the subscriber module, the resource references of the subscriber module and a predictable variable (col. 8, lines 50-59).

As per claim 38, Parker teaches the equipment is a Pay-TV decoder or a computer to which the security module is connected (col. 12, lines 60-65).

As per claim 39, it is rejected for the same reasons as claim 1.

As per claim 40, Parker teaches a subscriber module of the "SIM card" type connected to a mobile equipment (col. 1, lines 50-55).

Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Parker and Vatanen as applied to claim 1 and in further view of USP Application Publication 2003/0041125 to Salomon.

As per claim 37, Parker and Vatanen are silent in disclosing the subscriber module transmits to the control server, via the mobile equipment and the mobile network, a confirmation message when the subscriber module has received the cryptogram, said message confirming the correct reception and the adequate processing of the cryptogram by the subscriber module. Salomon teaches the subscriber module transmits to the control server, via the mobile equipment and the mobile network, a confirmation message when the subscriber module has received the packet, said message confirming the correct reception and the adequate processing of the cryptogram by the subscriber module (0056). Receipt messages or as they are usually to in the art, acknowledgement messages (ACK), are notoriously well known in the art of computer communication. ACK are used to ensure proper and reliable communication between two devices. The ACK serves to let the sender know the

packet was received by the recipient so the sender can timely conclude the communication. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the acknowledgement messages of Salomon in the method of activation of Parker and Vatanen so server can know that the phone received the data without error. Any type of computer communication method can benefit from ACK messages.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431